Cécile Pierrot

Cryptographer

Loria, Campus Scientifique
54506 Vandoeuvre-lès-Nancy
✉ *cecile.pierrot@inria.fr*
🖱 *https://almasty.lip6.fr/~pierrot/*
French citizenship

Research Positions

Since 2018 **Associate Professor (chargée de recherche to be more accurate), INRIA Nancy**, *Caramba Team*, INRIA - Institut de Recherche en Informatique et en Automatique, Nancy, France.

2017 **Postdoctoral position at CWI, Amsterdam**, *Cryptology Group, Ronald Cramer's team*, Centrum voor Wiskunde & Informatica, Amsterdam, The Netherlands.

Oct 2016 - Dec 2016 **Postdoctoral position at Mathematical Institute, Oxford**, *Cryptography and Number Theory Research Groups, under the supervision of Roger Heath-Brown, Mathematical Institute*, University of Oxford, United-Kingdom.

Education

2013 - 2016 **Ph.D. in Computer Science : The discrete logarithm problem in finite fields**, *Laboratoire d'Informatique de Paris 6*, UPMC, Sorbonne-Universités, Paris, France.
Funded by : DGA (French Ministry of Defense) and CNRS (French Center for Scientific Research).
Advisor : Antoine Joux.
Reviewers : Reynald Lercier and Alfred Menezes.
Defended on Nov 25th, 2016 in front of : Daniel Augot, Ronald Cramer, Guillaume Hanrot, Antoine Joux, Reynald Lercier, Ariane Mézard and David Naccache.

2012 - 2013 **Master's Degree in Mathematics : Algebra and its application to Symbolic Computation and Cryptography**, Université de Versailles, Saint-Quentin, France.
Best master average in this section.
Research internship in PRiSM laboratory, UVSQ, under the supervision of Antoine Joux.

2008 - 2011 **Bachelor's Degree in Fundamental Mathematics and Probability**, UPMC, Sorbonne-Universités, Paris, France.

Academic prizes

2017 **Cyber security award**, *Cercles K2*, French award attributed for an outstanding PhD thesis in IT security related issues.

2012 **Student excellence award and grant**, *Fondation mathématique Jacques Hadamard*, .

2006 **1st accessit at the Concours Général de Géographie**, *Lycée Louis-le-Grand*.

Publications

4 Articles published in journals with review committees

Pierrot, Wesolowski **Malleability of the Blockchain's Entropy**.
Cryptography and Communications, Springer, 2017

Joux, Pierrot **Nearly Sparse Linear Algebra, and applications to Discrete Logarithm Computations**.
Review Volume Contemporary Developments in Finite Fields and Applications, World Scientific Publishing Company, 2016

Joux, Pierrot **Technical history of discrete logarithms in small characteristic finite fields. The road from subexponential to quasi-polynomial complexity**.
Journal of Designs, Codes and Cryptography, 2016

Barbulescu, Pierrot **The Multiple Number Field Sieve for Medium and High Characteristic Finite Fields**.
London Mathematical Society Journal of Computation and Mathematics et présenté à ANTS 2014

4 Arcticles presented in international conferences with review committees

Pierrot, Wesolowski **Malleability of the Blockchain's Entropy**.
ArcticCrypt Conference 2016

Pierrot **The Multiple Number Field Sieve with Conjugation and General Joux-Lercier methods**.
Eurocrypt 2015

Joux, Pierrot **Improving the Polynomial time Precomputation of Frobenius Representation Discrete Logarithm Algorithms, Simplified Setting for Small Characteristic Finite Fields**.
Asiacrypt 2014

Joux, Pierrot **The Special Number Field Sieve in Finite Fields. Application to Pairing-Based Construction**.
Pairing 2013

1 Book chapter

Joux, Odlyzko, Pierrot **The Past, evolving Present and Future of Discrete Logarithm**.
Open Problems in Mathematical and Computational Science Book, Springer, 2014.

2 Dissemination articles

Joux, Pierrot **Discrétion Assurée**.
Gazette de la Société Mathématique de France, Avril 2015

Joux, Pierrot **La cryptographie à l'honneur : Diffie et Hellman, prix Turing 2015**.
1024, bulletin de la Société Informatique de France, Avril 2016

Scientific Communication

12 Presentations in International Conferences and Workshops

Paris, France **Malleability of the blockchain's entropy**, 01/05/2017.
Workshop WRONG, Invited Speaker

La Bresse, France **Le logarithme discret dans les corps finis**, 04/2017.
JC2, Invited Speaker

Porquerolles, France **Malleability of the blockchain's entropy**, 07/06/2016.
Yet Another Conference in Cryptography

Toulon, France **Résolution de problèmes d'algèbre linéaire presque creuse**, 06/10/2015.
JC2 (Coding and Cryptography Days)

Bordeaux, France **Discrete Logarithms in Medium Characteristic Finite Fields : Multiple Sieving and Fast Linear Algebra**, 28/09/2015.
Elliptic Curve Cryptography Conference

Kalamata, Greece **Nearly Sparse Linear Algebra and its application to Discrete Logarithms Computations**, 23/07/2015.
Applications of Computer Algebra Conference

Sofia, Bulgaria **The Multiple Number Field Sieve with Conjugation and Joux-Lercier Methods**, 27/04/2015.
Eurocrypt Conference

Clervaux, Luxembourg **Simplified settings for DLP in small characteristic finite fields**, 13/01/2015.
Early Symmetric Crypto Conference

Kaohsiung, Taiwan **Improving the polynomial time precomputation of Frobenius Representation Algorithms**, 09/12/2014.
Asiacrypt Conference

Gyeong-Ju, South Korea **The Multiple Number Field Sieve for Medium and High Characteristic Finite Fields**, 08/08/2014.
ANTS-XI Conference

Porquerolles, France **Medium and high characteristic DLP**, 12/06/2014.
Yet Another Conference in Cryptography

Ascona, Switzerland **On the power of V**, 08/05/2014.
Theoretical and Practical Aspects of the Discrete Logarithm Problem Conference

Grenoble, France **(S/M)NFS : DLP en moyenne et grande caractéristiques**, 25/03/2014.
JC2 (Coding and Cryptography Days)

Beijing, China **The Special NFS in pairing friendly finite fields**, 23/11/2013.
Pairing Conference

20 Talks at Seminars

Lyon **Nearly Sparse Linear Algebra together with Cryptography**, 12/05/2017.
France LIP, ENS Lyon

Leiden **Discrete logarithm for pairing constructions**, 31/01/2017.
The Netherlands Bachelorseminarium algebra, meetkunde en getaltheorie, University of Leiden

Bristol **Public random number and cryptocurrencies**, 16/12/2016.
Royaume-Uni Crypto group, University of Bristol

Paris **Le logarithme discret dans les corps finis**, 25/11/2016.
France Laboratoire d'Informatique de Paris 6, UPMC

Limoges **Le logarithme discret dans les corps finis**, 13/11/2016.
France Xlim, Université de Limoges

Oxford **Nearly Sparse Matrices**, 12/10/2016.
United-Kingdom Mathematical Institute, Oxford University

Grenoble **Malleability of the Blockchain Entropy**, 15/09/2016.
France Séminaire Casys, Grenobles-Alpes University

Nancy **About Bitcoin and public random number generation**, 13/06/2016.
France Caramba Seminar, Loria

Grenoble **Résolution de problèmes d'algèbre linéaire sur des matrices presque creuses**, 11/02/2016.
France Séminaire Casys, Grenobles-Alpes University

Suzhou, **Simplified Setting for Small Characteristic Discrete Logarithms**, 11/12/2016.
China Number Theory Seminar, Soochow University

Versailles **Le simply : log discret en petite caractéristique**, 26/11/2015.
France Crypto Seminar of Versailles Mathematic Laboratory

Rennes **Log discret par méthode simplifiée**, 20/11/2015.
France IRMAR Crypto Seminar

Paris **Algèbre linéaire creuse ou dense ?**, 25/06/2015.
France Seminar of Télécom Paris

Paris **DLP in medium characteristic finite fields**, 26/05/2015.
France Masterclass of Silvio Micali's Colloquium

Paris **Le logarithme discret dans les corps finis**, 02/02/2015.
France Laboratoire d'Informatique de Paris 6

Paris **Le problème du logarithme discret**, 24/04/2014.
France Institut Mathématique de Jussieu

Nancy **Crible spécial par corps de nombres pour les corps finis issus de couplage**, 06/12/2013.
France Seminar of Caramel's Team, Loria

Lausanne, **SNFS and application to pairing-based construction**, 14/11/2013.
Switzerland LACAL Seminar, EPFL - Ecole Polytechnique Fédérale de Lausanne

Versailles **Logarithme discret dans $\mathbf{F}_{p^n}$: crible spécial par corps de nombres**, 16/10/2013.
France PRiSM Laboratory, UVSQ

Versailles **Soutenance de M2 : Le logarithme discret dans les corps finis**, 24/09/2013.
France Laboratoire de Mathématique de Versailles

Scientific commitments

Involvement in conferences and reviewing

Eurocrypt 2017 **Reviewer**.

PKC 2017 **Reviewer**.

JCSS **Reviewer**, *Journal of Computer and System Sciences*, 2016.

Latincrypt 2015 **Program Committee Member**, *Conference in collaboration with IACR (International Association for Cryptology Research)*, Guadalajara City, Mexico.

IEEE **Reviewer**, *Transactions on Information Theory*, 2015.

JMC Journal **Reviewer**, *Journal of Mathematical Cryptology*, 2015.

Pairing 2013 **Session Chair**, *The 6th International Conference on Pairing-Based Cryptography*, Beijing.

Research administration tasks

2014 - 2016 **Elected representative of the PhD students at the Laboratory board meetings**, *2 elected delegates for 250+ PhD students*.

2013 - 2016 **Member of the Organisation Committee of the Colloquium**, *One famous invited speaker per month*.

Teaching qualifications and experience

Spring 2016 **Supervision of projects**, *UPMC - Sorbonne Universities*.
Third year (Licence 3) Mathematics Major course : RSA and Factorisation (6h)

Fall 2015 **Teaching Assistant**, *UPMC - Sorbonne Universities*.
First year (Licence 1) Computer Science Major course : Elementary programming – in Python (58h)

Spring 2015 **Lectures and Teaching Assistant**, *UPMC - Sorbonne Universities*.
Fourth year (Master 1) Computer Science Major course : Number representation and algorithmic (10h)

Fall 2014 **Teaching Assistant**, *UPMC - Sorbonne Universities*.
First year (Licence 1) Computer Science Major course : Elementary programming – in Python (58h)

Spring 2014 **Teaching Assistant**, *UPMC - Sorbonne Universities*.
Second year (Licence 2) Computer Science Major course : Types and data structure (22h),
First year (Licence 1) Computer Science Major course : C Language for beginners (42h)